在Prime合作布建(PCP)中使用備用名稱指南生成CSR

目錄

簡介

本文說明如何在prime布建中產生憑證簽署請求(CSR)以允許使用替代名稱。

必要條件

需求

— 證書頒發機構(CA)需要對您從PCP生成的證書進行簽名，您可以使用Windows伺服器，或者讓CA對其進行聯機簽名。

如果您不確定如何讓證書由CA線上資源簽署，請參閱下面的連結

https://www.digicert.com/

— 需要對Prime調配的命令列介面(CLI)進行根訪問。根訪問許可權在安裝時生成。

> **附註**：有關PCP版本12.X及更高版本，請參閱本文檔底部的進一步說明

採用元件

Prime合作布建

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

這將允許您出於業務目的使用多個域名伺服器(DNS)條目使用同一證書訪問Prime合作調配

(PCP)，並且在訪問網頁時不會遇到證書錯誤。

程式和步驟

撰寫本檔案時，您只能從圖形使用者介面(GUI)產生沒有替代名稱的CSR，以下是完成此任務的說明。

步驟1.以超級使用者身份登入PCP

步驟2.使用**input cd**/opt/cupm/httpd/導航到/opt/cupm/httpd/

步驟3.型別**:vi san.cnf**

> **附註**：這將建立一個名為san.cnf的新檔案，該檔案此時為空

步驟4.按**I**以插入（這將允許編輯檔案），並將下面的內容複製貼上到灰色欄位中

另請注意，DNS底部的專案。1 = pcptest23.cisco.ab.edu是將用於CSR的主DNS專案，DNS.2將是輔助專案； 這樣，您可以訪問PCP並使用其中一個DNS條目。

在此範例中複製/貼上後，請刪除包含您應用所需範例的pcptest範例。

```
[ req ] default_bits = 2048 distinguished_name = req_distinguished_name req_extensions = req_ext [
req_distinguished_name ] countryName = Country Name (2 letter code) stateOrProvinceName = State or Province Name
(full name) localityName = Locality Name (eg, city) organizationName = Organization Name (eg, company) commonName =
Common Name (e.g. server FQDN or YOUR name) [ req_ext ] subjectAltName = @alt_names [alt_names] DNS.1 =
pcptest23.cisco.ab.edu DNS.2 = pcptest.gov.cisco.ca
```

步驟5.鍵入：**esc**，然後**鍵入：wq!** （這將儲存檔案和剛才所做的更改）。

步驟6.重新啟動服務，配置檔案才能正確生效。型別：**/opt/cupm/bin/cpcmcontrol.sh stop**

鍵入**/opt/cupm/bin/cpcmcontrol.sh status**以確保所有服務都已停止

步驟7.鍵入以下命令以允許服務重新啟動：**/opt/cupm/bin/cpcmcontrol.sh start**

步驟8.您應該仍在**/opt/cupm/httpd/**目錄中，可以鍵入**pwd**以查詢您的當前目錄以進行確定。

步驟9.運行此命令以生成私鑰和CSR。

openssl req -out PCPSAN.csr -newkey rsa:2048 -nodes -keyout PCPSAN.key -config san.cnf

```
[root@ryPCP11-5 httpd]# openssl req -out PCPSAN.csr -newkey rsa:2048 -nodes -keyout private.key -config san.cnf
Generating a 2048 bit RSA private key .........+++ .........+++ writing new private key to 'private.key' ----- You
are about to be asked to enter information that will be incorporated into your certificate request. What you are
about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some
blank For some fields there will be a default value, If you enter '.', the field will be left blank. ----- Country
Name (2 letter code) []:US State or Province Name (full name) []:TX Locality Name (eg, city) []:RCDN Organization
Name (eg, company) []:CISCO Common Name (e.g. server FQDN or YOUR name) []:doctest.cisco.com [root@ryPCP11-5 httpd]#
```

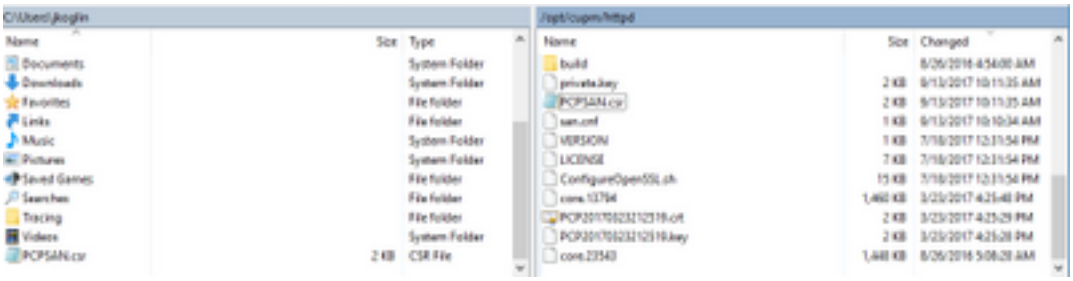
生成CSR並驗證CSR是否包含正確的替代名稱，請鍵入以下命令

openssl req -noout -text -in PCPSAN.csr | grep DNS

```
[root@ryPCP11-5 httpd]# openssl req -noout -text -in PCPSAN.csr | grep DNS DNS:pcptest23.cisco.ab.edu,
DNS:pcptest.gov.cisco.ca [root@ryPCP11-5 httpd]#
```

> **附註**：如果DNS條目與步驟4中所示的相同，您應該會看到與步驟4中所輸入相同的條目。對其進行驗證後，繼續下一步

步驟10.使用名為winscp或filezilla的程式作為根使用者連線到PCP，然後導航到/**opt/cupm/httpd/**目錄，並將.csr從PCP伺服器移動到您的案頭。



步驟11.使用您的CA簽署CSR，並使用Windows伺服器或通過第三方供應商（如DigiCert）線上。

步驟12.在Gui中安裝PCP證書，導航：**Administration>Updates>SSL Certificates。**

步驟13.透過瀏覽器安裝憑證，每個瀏覽器的參考資料如下。

Google Chrome:

https://www.tbs-certificates.co.uk/FAQ/en/installer_certificat_client_google_chrome.html

Internet Explorer:

http://howtonetworking.com/Internet/iis8.htm

https://support.securly.com/hc/en-us/articles/206082128-Securly-SSL-certificate-manual-install-in-Internet-Explorer

Mozilla Firefox:

https://wiki.wmtransfer.com/projects/webmoney/wiki/Installing_root_certificate_in_Mozilla_Firefox

步驟14.在伺服器和瀏覽器上安裝證書後，清除快取並關閉瀏覽器。

步驟15.重新開啟URL，不應遇到安全錯誤。

進一步說明

附註：PCP版本12.x及更高版本需要使用TAC來提供CLI訪問許可權，因為此許可權受到限制。

請求CLI訪問的過程

步驟1.登入到PCP GUI

步驟2.導航到**Administration>Logging and Showtech>Click on troubleshooting account>建立使用者ID並選擇需要root訪問許可權的合適時間。**

步驟3.向TAC提供質詢字串，他們會為您提供密碼（此密碼將很長，不用擔心會起作用）。

```
Example:
AQAAAAEAAAC8srFZB2prb2dsaW4NSm9zZXBoIEtvZ2xpbgAAAbgBAAIBAQIABAAA FFFFEBE0
AawDAJEEAEBDTj1DaXNjb1N5c3RlbXM7T1U9UHJpbWVDb2xsYWJvcmF0aW9uUHJv FFFFEB81
dmlzaW9uaW5nO089Q2lzY29TeXN0ZW1zBQAIAAAAAFmxsrwGAEBDTj1DaXNjb1N5 FFFFEB8A
c3RlbXM7T1U9UHJpbWVDb2xsYWJvcmF0aW9uUHJvdmlzaW9uaW5nO089Q2lzY29T FFFFEAD0
eXN0ZW1zBwABAAgAAQEJAAEACgABAQsBAJUhvhhxkM6YNYVFRPT3jcqAsrl/1ppr FFFFEB2B
yr1AYzJa9FtO1A4l8VBlp8IVqbqHrrCAIYUmVXWnzXTuxtWcY2wPSsIzW2GSdFZM FFFFE9F3
LplEKeEX+q7ZADshWeSMYJQkY7I9oJTfD5P4QE2eHZ2opiiCScgf3Fii6ORuvhiM FFFFEAD9
kbbO6JUguABWZU2HV0OhXHfjMZNqpUvhCWCCIHNKfddwB6crb0yV4xoXnNe5/2+X FFFFEACE
```

```
7Nzf2xWFaIwJOs4kGp5S29u8wNMAIb1t9jn7+iPg8Rezizeu+HeUgs2T8a/LTmou FFFFEA8F
Vu9Ux3PBOM4xIkFpKa7provli1PmIeRJodmObfS1Y9jgqb3AYGgJxMAMAAFB6w== FFFFEAA7
DONE.
```

步驟4.註銷當前使用者，並使用您建立的使用者ID和TAC提供的密碼登入。

步驟5.導覽至Troubleshooting Account>>Launch>>Click on Console Account，然後建立您的cli使用者id和密碼。

步驟6.現在以您建立的使用者身份登入到PCP，並執行本文檔中所述的初始步驟。

附註：PCP版本12.x及更高版本需要先輸入命令**sudo**，然後所有指令才能使其工作。因此，在步驟9中，命令將是**sudo openssl req -out PCPSAN.csr -newkey rsa:2048 -nodes -keyout PCPSAN.key -config san.cnf。若要確認DNS，接著您將在PCPSAN.csr中使用sudoopenssl req -noout -text** 指令 **| grep DNS**